

CLAIMS

What is claimed is:

1. A method comprising:
receiving first data to be blindly signed;
establishing parameter data for use with signature generating logic that encrypts data based on a Jacobian of at least one curve, said parameter data causing said signature generating logic to select at least one Gap Diffie-Hellman (GDH) group of elements relating to said curve;
determining private key data and corresponding public key data using said signature generating logic; and
generating second data by signing said first data with said private key data using said signature generating logic, said second data having a corresponding blind digital signature.

2. The method as recited in Claim 1, further comprising
generating said first data by:

digitally signing a message $m \in \{0, 1\}^*$,

determining $h = h(m) \in G$,

selecting a random $r \in \mathbb{Z}_p^*$ and

setting $h' = r \cdot h \in G$, wherein said first data includes h' .

3. The method as recited in Claim 2, wherein said parameter data establishes a base group G of order p and generator g as system parameters for said signature generating logic.

1 4. The method as recited in Claim 3, wherein determining said private
2 key data and said public key data includes:

3 picking $x \in \mathbb{Z}_p^*$, and

4 computing $v \leftarrow g^x$, wherein said public key data includes v and said private
5 key data includes x .

6
7 5. The method as recited in Claim 4, wherein generating second data
8 by signing said first data further includes:

9 signing h' by computing $\sigma' = x \cdot h' \in G$.

10
11 6. The method as recited in Claim 5, further comprising:
12 determining if said blind digital signature is valid.

13
14 7. The method as recited in Claim 6, wherein determining if said blind
15 digital signature is valid further includes:

16 obtaining a GDH signature on h by computing $\sigma = r \cdot \sigma' \in G$ where $r' = r^{-1}$

17 mod p and $\sigma = x \cdot h \in G$ is a valid GDH signature on m ; and

18 determining if (g, v, h, σ) is a valid Diffie-Hellman tuple

19
20 8. A computer-readable medium having computer-implementable
21 instructions for performing acts comprising:

22 receiving first data to be blindly signed;

23 configuring signature generating logic using parameter data so as to be
24 capable of encrypting data based on a Jacobian of at least one curve, said
25

1 parameter data causing said signature generating logic to select at least one Gap
2 Diffie-Hellman (GDH) group of elements relating to said curve;

3 determining private key data and corresponding public key data using said
4 signature generating logic; and

5 generating second data by signing said first data with said private key data
6 using said signature generating logic, said second data having a corresponding
7 blind digital signature.

8
9 9. The computer-readable medium as recited in Claim 8 having
10 computer-implementable instructions for performing further acts comprising:

11 generating said first data by digitally signing a message $m \in \{0, 1\}^*$,
12 determining $h = h(m) \in G$, selecting a random $r \in \mathbb{Z}_p^*$ and setting $h' = r \cdot h \in G$,
13 wherein said first data includes h' .

14
15 10. The computer-readable medium as recited in Claim 9, wherein said
16 parameter data establishes a base group G of order p and generator g as system
17 parameters for said signature generating logic.

18
19 11. The computer-readable medium as recited in Claim 10, wherein
20 determining said private key data and said public key data further includes:

21 picking $x \in \mathbb{Z}_p^*$, and

22 computing $v \leftarrow g^x$, wherein said public key data includes v and said private
23 key data includes x .

1 12. The computer-readable medium as recited in Claim 11, wherein
2 generating second data by signing said first data further includes:

3 signing h' by computing $\sigma' = x \cdot h' \in G$.

4
5 13. The computer-readable medium as recited in Claim 12, having
6 computer-implementable instructions for performing further acts comprising:

7 determining if said blind digital signature is valid.

8
9 14. The method as recited in Claim 13, wherein determining if said blind
10 digital signature is valid further includes:

11 obtaining a GDH signature on h by computing $\sigma = r \cdot \sigma' \in G$ where $r' = r^{-1}$
12 $\text{mod } p$ and $\sigma = x \cdot h \in G$ is a valid GDH signature on m ; and

13 determining if (g, v, h, σ) is a valid Diffie-Hellman tuple

14
15 15. An apparatus comprising:

16 memory configured to store first data that is to be blindly signed; and

17 signature generating logic operatively coupled to said memory and
18 configured according to parameter data so as to be capable of encrypting data
19 based on a Jacobian of at least one curve, said parameter data causing said
20 signature generating logic to select at least one Gap Diffie-Hellman (GDH) group
21 of elements relating to said curve, determine private key data and corresponding
22 public key data, and generate second data by signing said first data with said
23 private key data, said second data having a corresponding blind digital signature.

24

25

1 16. The apparatus as recited in Claim 15 wherein said first data is
2 generated by a second logic operatively coupled to said first logic by digitally
3 signing a message $m \in \{0, 1\}^*$, determining $h=h(m) \in G$, selecting a random
4 $r \in Z_p^*$ and setting $h'=r \cdot h' \in G$, wherein said first data includes h' .

5
6 17. The apparatus as recited in Claim 16, wherein said parameter data
7 establishes a base group G of order p and generator g as system parameters for
8 said signature generating logic.

9
10 18. The apparatus as recited in Claim 17, wherein said signature
11 generating logic is further configured to determine said private key data and said
12 public key data by picking $x \in Z_p^*$, and computing $v \leftarrow g^x$, wherein said public key
13 data includes v and said private key data includes x .

14
15 19. The apparatus as recited in Claim 18, wherein said signature
16 generating logic is further configured to generate said second data by signing h'
17 and computing $\sigma' = x \cdot h' \in G$.

18
19 20. The apparatus as recited in Claim 15, wherein said memory and said
20 signature generating logic are provided within a computing device.
21
22
23
24
25